HOXHUNT

Phishing simulations with Microsoft Attack Simulator

Manual tools can identify human cyber-risk, but automation is needed to change behavior.

Time needed to send one phishing simulation manually

The end-to-end delivery is estimated to take 3-4 weeks while involving the admin, communications, translation, and pilot team.

Checklist for sending a phishing simulation with MS Attack Simulator	
1	**Create the template**: Create the phishing template to be used in the simulation, and validate the HTML used. Fix any formatting issues that might arise.
2	**Technical test**: Verify that links used in phishing simulation are not blocked in IE, Firefox, Chrome, and Edge browsers.
3	**First pilot test**: Review and send the simulation to a small test group (max 5 users) to test that the template works.
4	**Landing page**: Create and review the landing page in English. Request a review from corporate communication team.
5	**Translations**: Translate landing page to all other required languages.
6	**Standard response**: (Using Microsoft Power Apps) Create Standard Automatic Replies for the users who have successfully reported simulation.
7	**Second pilot test**: Send the simulation again to the test group to test that phishing templates, simulation URL, landing page and Standard Automatic Replies work.
8	**Create recipient groups**: Create O365 sub-groups of users who will receive the simulation. Microsoft has a limitation of sending simulation to only 500 users in a group. Create sub-groups with a maximum of 500 users per group.
9	**Inform service-desk and IT**: Communicate the simulation launch date and details to service desk and IT so that they are prepared to address any user queries.
10	**Launch campaign**: Launching phishing campaign to all employees (all recipient groups).
11	**Include feedback collection**: Collect feedback and NPS score from the recipients.
12	**Report out**: Monitor and report out the status for the next week.
13	**Review employee feedback**: Go through the feedback given by the participating employees.
14	**Retrospective**: Gather lessons learned during the process and from employee feedback.

Choose the right phishing solution for your needs

Hoxhunt shines with its world-class continuous AI-powered phishing training that delivers high user engagement. The training makes organizations more resilient by increasing the rate and accuracy of real-threat reporting.

In addition to continuous training, self-configured benchmark phishing campaigns can be scheduled to test the organization's resilience against selected templates.

Advanced Phishing Training

Adaptive, continuous training turns employees into expert phishing-detectors that protect your company.

The simulations are intended to teach participants to recognize phishing attacks and report them.

- Adaptive training adjusts simulation selection and timing for each user.
- Automatic sending throughout the year. Builds muscle-memory to report suspicious emails.
- Simulations are personalized to each user's language, region and job function and adjusted for their skill.
- Micro-training on both phishing report success and failure.
- Gamified experience keeps users engaged with training.

Benchmark phishing simulations

One-off phishing simulations that are sent manually to test end-users.

The simulations measure how prone your organization is to phishing attacks.

- Scheduled campaign to selected recipients with set simulation selection.
- Simulations are personalized to each user's language.
- Measure the baseline phishing risk of your organization's various departments.
- Benchmark your risk level against industry-peers and companies across the Hoxhunt network.

Configure once, use without limits.

Once you have been onboarded onto Hoxhunt, phishing training will be always-on and runs automatically. One-off benchmark tests can be sent without any additional configuration.